Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures

Ahmad Mtair AL-Hawamleh
Department of Electronic Training,
Institute of Public Administration, Riyadh, Saudi Arabia

***Abstract*—The Internet interconnections' exponential growth has resulted in an increase in cyber-attack occurrences with mostly devastating consequences. Malware is a common tool for performing these attacks in cyberspace. The malefactors would either exploit the present weaknesses or employ the distinctive characteristics of the developing technologies. The cybersecurity community should increase their knowledge on the types and arsenals of cyber-attacks, and security measures against cyber-attacks should be in place as well. Also, advanced and effective malware defense mechanisms should be established. Hence, this study reviews cyber-attack types, measures and security precautions, and professional extrapolations on cyber-attacks future and the associated security measures. Semi-structured interviews were performed, involving five IT managers and nine Cybersecurity Consultants, to obtain the data. The study findings demonstrate prevention as key for data breach risk prevention. Knowledge of common attack methods and the use of cybersecurity software can facilitate individuals and organizations in thwarting hackers and in preserving their data privacy. Two-factor authorization by consumers and new back-end security protocols and security methods, including Artificial intelligence (AI) application, will encumber hacking attempts.**

***Keywords*—Cybersecurity; cybercriminals; cyber-attacks; cybersecurity techniques; security precautions**

I. Introduction

The last 20 years have seen the emergence of the Internet as key to global communication, making the Internet today an important part of the life of people globally. Worldwide, [1] reported that there were more than 3 billion internet users, and such number of users has been greatly factored by the ubiquity and low cost of the Internet. Through the immense global network made possible by the Internet, billions of dollars have been generated each year, adding to the global economy [2, 3]. Today, interactions and many other activities of various types are being carried out in cyberspace [3, 4], like financial transactions between business parties and casual communication between individuals [5, 6]. The cyberspace controls, manages and exploits vital and sensitive infrastructures and systems, but the cyberspace can also be made up of such infrastructures and systems [7].

The cyberspace is where varied aspects of citizens' lives are interconnected, and so, as indicated by [8], the conditions of the cyberspace will directly affect the lives of the citizens [8]. Today, cyberspace has presented new security challenges to governments. As reported by [9], cyber-attacks and their effects have been the subject of concern among analysts since the last decade. Cyber-attacks undeniably lead to damages, physical and/or economic, and there have been cases where the damages were so widespread and severe, as can be exemplified by virus attacks on stock market of a country, resulting in a crash or a loss of colossal amount of money, or virus attacks on a power plant system leading to a massive explosion loss of lives and properties, just to name a few [10, 11].

The advent of the Internet and the current digital transformation have made cybersecurity a serious matter to experts and all other involved parties. Today, people are increasingly dependent on computer systems, the Internet, and wireless networks (e.g., Bluetooth and WiFi) [12], as can be observed by the increasingly common dependence of people towards smart devices like smartphones and the Internet of Things. In other words, people today are more at risk of being victims to cyber-attacks. Meanwhile, as reported by [13], the discovery of malicious activities on the network has been too common. In general, detection of intrusion has been reactive in nature, and the reaction is only to certain patterns or observed anomalies. However, scholars including [3] and [14] mentioned the need to employ a proactive approach instead, that is, to react to these intrusions before they manage to cause any harm. Somehow, it appears that work and advancement in predictions, measures and security precautions concerning cyber security remain obscure, but, recently, the efforts seem to be gradually gaining momentum [3, 14, 15].

Cyber-attacks are becoming more complex and severe as time passes [16]. Currently, only little is understood pertaining to the different types of cyber-attacks, how these attacks spread, and the current security precautions against them. As such, many organizations/countries have fallen victim to these attacks. Meanwhile, security measure development needs comprehensive understanding of these attacks, and so, a complete listing and classification of cyber-attacks is a crucial element of cyber security initiatives. The present study seeks to describe the different kinds of cyber-attacks, measures and security defenses against them, while also predicting future cyber-attacks. Some security measures are proposed, to facilitate programmers in their development of security devices and mechanisms according to the mode of attack.

II. Related Works

A. Cybersecurity

Cybersecurity entails a bulk of practices, technologies, and processes specifically developed to safeguard the data, networks, programs, and devices of people and enterprises from attacks [3], [14]–[18]. Meanwhile, financial, corporate, government, military, and medical organizations generally gather, process, and store data in substantial amounts on computers and other devices. Some of these gathered data

can be sensitive data like personal data, financial data, and intellectual property, and so, access to such data requires authorization because negative consequences could result when these data are accessed by unauthorized parties [15, 19, 20]. Therefore, for these organizations, cybersecurity is a crucial matter [19]–[22].

In business transactions, sensitive data is transferred to other devices across networks. Appositely, cybersecurity encompasses the discipline for safeguarding the information and the applied systems in its process or storage [23]–[26]. In this regard, firms that are responsible to protect the information on financial records, health, and national security are obliged to take measures to safeguard their sensitive business and personnel information, especially now that cyber-attacks have increased in terms of volume and superiority [23]–[26].

Through a solid cybersecurity strategy, an appropriate security mechanism can be achieved, and this mechanism could effectively deter malicious attacks that generally would attempt to access, modify, erase, extinguish or extort the systems and sensitive data of persons or organizations [27]–[29]. Additionally, cybersecurity could deter attacks that could incapacitate or mess up the operations of a device or system [27]–[29].

B. Cybercriminals

Cybercrime relates to criminal activity involving a computer, networked device or a network [30]–[34]. In general, cybercrimes are executed by cybercriminals for the purpose of making personal gain [30]–[34]. However, there are cybercrimes performed for the purpose of damaging or disabling computers. There are also those who utilize computers or networks for the purpose of disseminating malware, and also for dispersing prohibited information, images or other materials [30]–[34].

Cybercrime was defined by the Council of Europe Convention on Cybercrime as a vast gamut of malicious activities, and among these activities are unlawful data interception, copyright infringements, and system intrusions, that impair the integrity and availability of the network [35, 36]. The USA is a signatory to this council [35, 36].

The internet connectivity is a common availability today as it is a requirement to various daily undertakings. However, such availability has caused cybercrime activities to thrive as the culprit could commit the crime without having to be physically present [37]. Fraud, money laundering, cyberbullying and cyber stalking are among the examples of commonly committed cybercrimes, and these crimes are further facilitated by the speed and convenience of the internet, and the anonymity and borderless reachability that the Internet is offering [23, 28, 36, 37].

Cybercrimes may be executed by persons or groups with fairly little technical skills. Equally, the crimes may be committed by extremely structured global criminal groups involving skilled developers and other experts. Also, it is common to see cybercriminals operating in countries that have no or weak cybercrime laws so that they could not be easily detected or prosecuted [38, 39].

C. Cyber Attacks

A cyber-attack is an intentional and malicious effort made by a person or an organization to break the information system of others [40]. The attack is usually economically driven, but there are also attacks that involve data or information stealing, modifying or destruction. In other words, among the goals of attack include to break the system, or to steal, modify or destroy the data or information of others [3, 15, 39, 40].

Cyber-attacks are more and more common these days. Furthermore, the Cisco Annual Cybersecurity Report [41] has relevantly indicated that the advent of network-based ransomware worms has allowed attackers to launch campaigns without the need for human involvement. Also, security events nowadays have become more intricate and more copious [41]. Moreover, businesses today face cyber-attacks on a daily basis; it was mentioned by the then CEO of Cisco (Mr. Chambers) that businesses can be classed into two groups; One comprises those that have been hacked, and the other comprises those that are still unaware of the fact that they have been hacked [42].

Cyber-attacks generally occur in six forms namely: Malware, Phishing, Denial of Service (DoS), Man-in-the-Middle (MitM), Password Spraying, and Cross-site Scripting (XSS) [40]–[49]. Each of these attack types is described as follows:

1) Malware: Malware encompasses malicious code or malicious software, and it is essentially a program that is covertly implanted inside a system with the purpose of disrupting the data so that the data would lose their integrity, confidentiality, or accessibility [50]. Malware is regarded as a major external threat to systems as it can affect the systems' operation [40, 43, 50]. Malware can cause widespread damage and disruption, and significant efforts would be required to fix this malware problem. Malware comes in various forms including Trojans, virus, worms, spyware and ransomware [40, 43, 50]. The details are as follows:

- Trojans: This type of malware is also known as Trojan horse, and encompasses a seemingly legitimate and safe file, program, or piece of code (but indeed a malware) [43, 51]. Usually, Trojans are bundled and transported within an authentic software, and are created for spying on or for stealing data from victims. Trojans display themselves as genuine files, and so, victims would be misled to click, open, or install these Trojans (without knowing). Upon installation, many Trojans will download other malware to spy on the victim or cause other types of harm.
- Viruses: Viruses generally will attach themselves to the order of initialization, and these viruses would replicate themselves to infect other codes within the computer system [40, 51, 52]. They also could attach themselves to executable code or link themselves with a file through forming a virus file with a similar name but with an extension [51,52]. This file is a decoy that transports the virus [40, 51, 52].
- Worms: Worms encompass self-contained programs spreading across networks and computers [43, 51, 53]. Frequently installed via email attachments, worms would dispatch a copy of themselves to all contacts

in the affected computer email list [53]. Usually, worms are used by perpetrators to overload an email server and generate a denial-of-service attack. However, worms don't attack the host like viruses do [40, 53].

- Spyware: This type of malware entails a program that attackers use to gather information relating to users, their systems or browsing routines, sending the data to a remote user [54]. The obtained information can be used by the attacker to blackmail the user. Also, the attacker could download and install other malicious programs from the web [40, 43, 51, 54].

- Ransomware: Ransomware is a very common attack method with the ability to inhibit or restrict the access of users to their system [55]. It also may instruct users to pay a certain amount of ransom using online payment methods [56], which generally would involve the use of virtual currencies like bitcoins, before they could re-access their system or data. Ransomware gets into computer networks; through the use of public-key encryption, ransomware encrypts the files, and this encryption key remains with the server of the cybercriminal [56]. Encryption is used by cyber criminals to detain the data, and the data owner has to pay a certain amount of ransom to get the private key [40, 43, 55, 56].

2) Phishing: Phishing is an activity of transmitting deceitful communications through seemingly reputable emails [45, 47]. It is common to see these emails demonstrating legitimacy but they actually link the receiver to a malicious script or file [45]. Through this script or file, the attackers could gain access to the device of the victim and gain control over it. Consequently, the attacker could also insert malicious scripts/files, and extract sensitive data like user information, financial data, and so forth [45, 46]. Essentially, phishing is done to steal confidential data such as the victim's login information and credit card details.

3) Denial of service (DoS) and distributed denial-of-service (DDoS): DOS attacks involve flooding the systems, servers, and/or networks with traffic for the purpose of overloading the resources and bandwidth, resulting in failure of the system in meeting valid requests [48]. DoS attacks can be simultaneously executed by various computers at one specific time and this is called Distributed Denial-of-Service (DDoS) attack [34, 48]. Dealing with DDoS attacks can be very challenging because attackers can come from various IP addresses globally, making it very difficult for network administrators to determine the attack source [30, 48].

4) Man-in-the-middle (MitM): Man-in-the-Middle (MitM) attack which is also called eavesdropping attack, involves hijacks by an attacker during a session between a trusted client and network server [47]. During the attack, the attacker's computer switches the IP address of a trusted client while the session is resumed by the server as the server thinks that it is still in communication with the client, not knowing that the client has been replaced with the attacker's computer [36, 47]. As an illustration: a client is in connection with a server when the computer of the attacker gains control over the client. The computer of the attacker then disconnects the client from the server. This is followed by the replacement of the client's IP address with that of the attacker's computer. The sequence numbers of the client are spoofed. The communication between the network server and the client resumes but the server does not know that it is no longer communicating with the client, but with the attacker's computer instead.

5) Brute-force and password spraying: Brute-force attacks generally involve attacks on a single account, whereby the attacker would test various passwords in the attempt of gaining access to an account [44]. This leads to recurrent failed logins [44, 57]. However, in general, modern cybersecurity protocols are able to identify such activity and will lock out an account following several failed login attempts within a short period of time [57].

However, the use of password spraying by attackers can overturn the standard protocols of cybersecurity [58]. Hence, the attacker would try to log on to several user accounts with the use of various passwords that are commonly used. Using a single password on several accounts before using another password on the exact accounts would prevent the standard lockout protocols from being activated. This way, the attacker could continue trying out more and more different passwords on the target account [44, 57, 58].

Owing to the failure of many users in adhering to best practices of password usage, the method of password spraying attacks are often successful. As reported in 2019, recognizable number arrangements like "12345", typical names of females like Jennifer, and the word "password" are among the most commonly used passwords among users [59, 60]. These, and other reported 200 easily guessed passwords have contributed to data breaches [59, 60]. Hence, attackers targeting a reasonably large number of usernames and utilizing a sufficiently large array of common passwords are likely to succeed in gaining access to some accounts [40, 43, 44, 59, 60].

6) Cross-site scripting (XSS): Cross-site scripting or XSS refers to a weakness of web security, allowing attackers to compromise the interactions of users with weak applications [49, 61]. The weakness of the user's system allows attackers to evade the exact origin policy that distinguishes websites [62]. The attacker could disguise as the user and perform any actions of the user and access all data of the user. Hence, the attacker may have complete functionality control over the application belonging to the user if the user has privileged access within the application [49, 61].

D. Cybersecurity Tools and Techniques

Today, the number of illegal attempts to gain access to private data has increased. These attempts are generally for stealing the data or for forcing users into information blackmailing. Such a situation has increased the importance of cybersecurity [3, 14, 15, 17, 18]. There are various methods being used in achieving cybersecurity. Among them include anti-virus, firewall, authentication, encryption and digital signatures. The details of each are as follows:

- Anti-Virus: A computer virus is generally an unwanted short program that prompts undesirable commands without user consent. An antivirus generally performs two tasks [15, 63]. The first task is to prevent the

installation of a virus in a system, and the second task is to scan the system to find out if there are viruses existing in a system [15, 63]. Most viruses are created to attack Windows operating systems because most users prefer to use Windows as their computing platform. However, there are also viruses created to attack Apple and Linux operating systems [63, 64].

- Firewall: Firewalls are created to provide an effective deterrent towards hackers' attempts to illegally access a computer upon its connection to the internet or to other network connections [65, 66]. Most operating systems are equipped with a firewall and the firewall is turned on by default. In addition to the default firewall, users could also install commercial firewalls if the default firewall does not provide sufficient protection or if it interferes with the user's legitimate network activities [65, 66].

- Authentication: Authentication is regarded as the basic method of cybersecurity. It provides a verification to user identity according to the records saved in the system's security domain [67]. Password technology is the most common security control method, but there are also other methods including SIM cards that are inserted into the cell phone of the user [67]–[69]. A SIM card has unique ID numbers, and during identification of certain cell phones, these numbers are transmitted over a secure communication line. During the process of authentication of a message, there may be eavesdropping attempts made by unauthorized parties, and it may be very difficult to counter these attempts. The transmission of password through an insecure medium may cause the password to be intercepted by fraudulent individuals disguising as the original user. Encryption can be used in dealing with this problem [67]–[69].

- Encryption: Encryption makes data incomprehensible and the right key is required to unlock it [70]. Resolving an encryption requires a resolution of intricate mathematical problems (e.g., factoring large primes) which is highly resource and time consuming [70, 71]. In the encoding and decoding of a message, a similar key is used in symmetric encryption, with security level similar to that of the key. Possible security risks are included alongside the key distribution. For asymmetric encryption, the public key is used in message encryption, while the private key is used in message decryption. For key distribution in today's security protocols, most employ asymmetric encryption [71].

- Digital signatures: Digital signatures can be formed from similar mathematical algorithms applied in asymmetric encryption [72]. Utilizing some information encoded with it, the user could perform a test to see if the key that he is in possession of, is private. Similar decryption can be obtained by the user through the attainment of a public key that will verify his (user) credentials [72, 73]. In general, this process is identical to that of public key encryption, and it operates based on the assumption that the authorized user is the only party in possession of private key [72, 73].

III. Methodology

The study data were obtained by way of semi-structured interviews. The interviews took 45 minutes, and the interviewees comprised five IT managers and nine cybersecurity Consultants. The interviewees were reached through email and they took part in the interviews willingly. They were asked about the types of cyber-attacks and the measures and security precautions to be taken to counter these attacks. The interviewees were also asked to make predictions concerning the future of cyber-attacks and relevant security measures. All interviews would be stripped off of the identifying details. The authors would discuss the extracted data until an agreement was reached.

IV. Findings and Discussions

The conducted interviews resulted in the understanding of cyber-attacks in terms of types and weapons. Also, the interviews provide the researcher with understanding of the measures and security precautions to counter cyber-attacks. Additionally, the interviewees made predictions concerning the future of cyber-attacks and the associated security measures. Accordingly, all interviews would be stripped off of identifying details. Any disagreements or concerns about the extracted data were discussed among the authors until a consensus was reached.

A. Types and Weapons of Cyber Attacks

There is an increasing number of people working from a distance or online since the year 2019 [74]. Consequently, as reported by the FBI, the number of cyber-attacks have increased by fourfold towards online activities [74]. Also, studies have shown an increase in the impact of successful cyber-attacks on organizations and their users each year [57, 74, 75].

As reported, about 197 million records became exposed in 2017 because of data breaches, and the number of exposed records rose to 37 billion in 2020 albeit the decrease in the overall number of data breaches [76, 77]. In countries such as the USA, IBM reported that organizations have to incur increasing cost when facing these attacks. As reported, the average cost of a data breach has risen to $8.64M in 2020 from $7.91M in 2018 [76, 77].

A lot of times, the success of cybercriminals in breaching organizations, also depending on the methods used, is facilitated or made possible by human error [3, 15, 17, 18]. For instance, the use of phishing may not be successful if the target victim did not click on the link provided. Also, some types of cyber-attacks exploit the gaps in user's efforts in data security, allowing these cybercriminals to gain access to sensitive data [3, 15, 17, 18].

In the interviews, the participants were asked on the types and weapons of cyber-attacks. One participant stated the following:

"Up to now, we are still facing some of the most common cyber-attacks, for example, Password Spraying Attacks, Ransomware, Denial of Service, and Malware Attacks too. Fortunately, there was no serious damage because we had been prepared – we invested a lot to build strategies against cyber-attacks. Still, we are not saying that we were unharmed at

all. The damage was there, of course. As precautions, we are consistent with our Advanced Persistent Threats (APT) audits. Also, we would always check our risky points."

Concerning the topic of ransomware, another interview participant stated the following:

"It appears that ransomware is not just a security incident. It has changed. Also, it is obvious that the present-day cybercriminals want to breach our data, and for that, they are teaming up with organized cybercrime groups to steal the data. Then, they encrypt on corporate servers. As a company, our focus is to regain our data. At the same time, we worry about which public is sharing the data. Cybercriminals use ransomware when they are under extreme pressure, and their targeted victim could be any party – individual, company, or government."

The interviewees were asked about Phishing techniques. The response of one interviewee is as follows:

"Phishing techniques involve emailing – the attacker would email thousands of deceitful messages to target victims. For instance, the victims would receive an email on receiving a handsome amount of money. Out of thousands of emails sent, certain fractions of target victims would fall for the scam. To increase the success rate, the attackers would use certain techniques, like mimicking the actual emails from a spoofed organization. For instance, PayPal. So, they would use similar phrasing, typefaces, logos, and signatures as PayPal's. So, the messages will look legitimate that the victim is less aware that they are being scammed or attacked."

One more interviewee offered an opinion regarding phishing, by stating the following:*"It is an increasingly common cyber threat today. As you can see, it is common to receive emails from what seems like a reputable source when it is really not the case. These criminals - they just want to steal sensitive data like your login and credit card information. They also want to install malware on your computer."*

The interviewees were asked on the subject of Distributed Denial of Service techniques used by cybercriminals. An interviewee responded by saying:

"Usually, a DDoS attack is done by a group of malware-infected host machines. The attacker controls these machines. We call these attacks the Distributed Denial of Service. This is because the attacks prevent the affected site from providing the user with the service it is supposed to provide, and therefore, the user cannot gain access to the site. The attack causes the victimized site to become flooded with illegal requests, and since the site has to answer to each request, its resources become all used up that it cannot serve users. A shutdown may happen to the site."

Research has confirmed that the attacks are essentially actions aimed at impairing a system or disturbing the normal operations of a system through the exploitation of the system's weaknesses through the use of different techniques and tools. Attacks are performed by attackers for different reasons like for gaining certain rewards or simply for personal satisfaction. The most commonly performed cyber-attacks on organizations today include Phishing, Password Spraying, Malware, Ransomware, Man-in-the-Middle (MitM), Denial of Service (DoS), and Cross-site Scripting (XSS).

B. Measures and Security Precautions against Cyber Attacks

Individuals and businesses could benefit from the use of cybersecurity measures as it could provide basic protection to both individuals and businesses from the most common cybersecurity risks. The tools and processes of cybersecurity measures are rather easy to follow. They include usage of strong passwords, a firewall, control of access, security software, intrusion monitoring, and increased awareness.

Most global data breaches (86%) are financially driven [78]. It is thus highly crucial for both individuals and businesses to be proactive in preserving their cybersecurity, considering that a cyber-attack can cost the company millions of dollars [78].

In order that their business data, cash flow and customers are safe online, businesses should employ various types of cybersecurity measures, so that risks from various sources could be averted. Among these sources include internet attacks, user faults, system or software defects and weaknesses, and subvert system or software features [79].

The interview participants were asked concerning their applied measures and security precautions in countering cyber-attacks. According to one of the participants:

"My organization uses two types of security measures and precautions – the traditional ones and the modern ones. The traditional ones include the common methods like IPS and IDS antivirus. They are used in different platforms. For modern measures, my organization uses anti-malware, DLP solutions and sandbox solutions."

On the same question, another interview participant responded by stating the following:

"In our organization, the main focus is to standardize and adapt all the used measures. The human factor is important as well. We believe that in modern cybersecurity measures, human capital is the most vital element. That is why our organization regularly trains the employees on how to avoid recurrent cyber-attacks."

The third participant offered his viewpoint as well. He said:

"I think that training programs are useful when you want to increase the awareness of personnel towards cybersecurity risks and cyber-attacks. Also, my organization is using security software and programs from different companies. This is to reduce the risks of cyber-attacks. For example, the antivirus and firewall software that my organization is using, was created by different companies. We feel that the risks and threats of cyber-attacks can be reduced this way."

For individuals, among the tips that they can follow in preserving their cybersecurity include creating a unique password for each account that they have and updating the password every three months, aside from constantly updating their software to prevent software flaws and to keep their software up to date. According to one participant:

"It is important that social media users make their account private. Also, they should not reveal their sensitive information in their posts. In fact, I think that social media users need to have knowledge about how to properly use the internet."

For protecting business data, among the tips for organizations to follow include the use of secure hardware, data backup and encryption, cybersecurity insurance, security-focused culture, and strong cybersecurity software. One participant accordingly reacted to these tips by saying: *"These steps will help in decreasing the risk and the business can operate in a smooth manner."*

Prevention is key to reducing the risk of a data breach. Through the use of cybersecurity software, and through having the knowledge of the common attack methods, both individuals and organizations could preserve the privacy of their data and inhibit hackers.

C. The Future of Cyber Attacks and Related Security Measures

In today's technology, cybersecurity is an integral element, amounting to approximately $250 billion in market value [80]. Like the general tech industry, there is a market for cybersecurity in nearly all industries, especially now that the amount of company information being stored online is increasing, and so is the demand for cybersecurity solutions to assure its security.

Leaks and hacks on a large scale have occurred in the last several years, and they have cost companies their customer's information and also their reputation [76]. For consumers, such occurrences have impaired their sense of safety and their security, and it could even disrupt their lives. Hackers seek leaked information as such information allows them to steal money and sensitive information from people.

In order to get access to lists of user accounts, hackers will go to major websites. However, hackers may face hurdles in their attempts to steal personal information of users from those sites. As stated by one participant of the interview:

"Our prediction is that cyber-criminals will learn new and innovative ways to attack people, their homes and devices, in their efforts of finding a path to your trustworthy corporate network."

Then, another participant added to the discussion by stating: *"Two-factor authorization is now commonly practiced by consumers. There are also new back-end security protocols and security methods. AI is one good example, and I am confident that AI has the ability to disable hacking attempts. Still, we should not say that everything is secure because we all know that hackers will keep finding ways around security structures. Hence, cybersecurity professionals must always be one step ahead."*

In discussing the topic of Ransomware, a participant said: *"Criminals have been making good profit through Ransomware these past several years. They would block users from using their computers and networks using some malicious software. These users are forced to pay large amounts of money or ransom to these criminals to regain their computer or network use. Unfortunately, we can expect that ransomware attacks will increase."*

It has been reported that the damages caused by ransomware had amounted to USD $11.5 billion in 2019 and the amount was expected to increase to USD $20 billion by 2022 [81].

On phishing attacks, a participant reacted by saying: *"Phishing attacks are increasing and it is increasingly more difficult to detect them. A good example is the MailChimp phishing campaign case. Hackers made use of affected accounts in MailChimp to distribute malicious emails with malware, and considering that MailChimp is a trusted and well-established email marketing provider, the emails were likely to bypass the spam filters and enter the inbox of the unwary receiver."*

Some experts agreed with the prediction that cybercrimes would cause financial damages amounting to $6 trillion by the end of 2022 [82]–[84]. Also, a cyber-attack would be expected to occur in every 11 seconds, as compared to one attack in every 19 seconds reported in 2019. Comparatively, in 2016, one cyber-attack occurred every 40 seconds [82]–[84].

The COVID 19 outbreak has forced many to work remotely. On this matter, a participant stated the following:

"COVID 19 has sped up the digital transformation of organizations and many employees have shifted to working from home. The problem with this situation is that, when working from home or remotely, employees are not safeguarded by corporate firewalls. Hackers could exploit the vulnerabilities that they discover in the gaps between people, their devices, and the corporate network. We can see that many employees are required to establish workloads in Cloud, and so, cloud-based security techniques are crucial in curbing the failing cybersecurity landscape. It is now necessary to work with cloud-native Identity and Access Management (IAM)."

As stated by another participant: *"For those who maintain cloud-based security, they have to have adequate ability in managing the infrastructure with the use of structured programs. We know that networks and application tiers are short-lived, and so, for any organization, their most crucial asset is probably their own data and the data of their customers. Therefore, I think that data-security on the cloud will be a main theme in the future."*

One participant viewed: *"cybersecurity as a highly viable career path."* In fact, it was predicted that the number of vacant cybersecurity jobs would increase by 35%, considering the increase in cyber-attacks and the shifts in tactics used by cybercriminals [85, 86]. In other words, cybersecurity is likely to become a sound career choice in the long run.

In terms of AI application, all interviewees agreed that it can effectively improve the security of cyberspace. Also, the options of AI systems should be fully used so that the most optimal level of cybersecurity could be achieved. One participant indicated that: *"the use of AI can allow the discovery of new and refined transformations in attack flexibility."* Notably, the old technology concentrates on the past and is mostly focusing on identified attackers and attacks. This can lead to the formation of blind spots in the detection of uncommon behavior in new attacks. For instance, privileged activity in an intranet can be monitored, and any discernible alteration in privileged access operations can signify a likely internal threat. For successful detection, the machine will strengthen the validity of the actions and increase its sensitivity for the detection of equivalent patterns in the future.

According to one participant: *"AI facilitates machine*

learning. It also helps the machine in detecting irregularities more effectively, and also in increasing the accurateness of operations. AI is particularly useful in dealing with more sophisticated cyber-attacks because the approaches used by hackers are increasingly more innovative these days."

One participant indicated that: *"the use of AI can increase network security, particularly through the ability of AI in detecting attacks and in responding to breaches."* For security groups, they could be overwhelmed by the amount of security alerts that they receive on a daily basis. Hence, the automatic detection and response towards threats can decrease their workload significantly. Also, they could more effectively detect the threats with the use of AI.

The formation and transmission of colossal amounts of security data on a daily basis would gradually impair the ability of security experts in quickly and reliably tracking and identifying the attack factors [87]. With the use of AI, the monitoring and detection of doubtful behavior could be expanded. This allows the network security personnel to effectively and promptly react to new situations.

The majority of participants agreed with the fact that in improving its response to threats, AI security systems have the ability to learn over time. Utilizing AI will facilitate the detection of threats following the application behavior and the entire network activity. The AI security system studies the standard network traffic and behavior, and over time, AI creates a reference point on what constitutes a normal pattern, and any divergences from the norm can be identified to determine attacks.

Considering the viewpoints of the participants in the interviews, it is clear that cybersecurity experts have to be consistently ahead of the cybercriminals. Also, the use of AI techniques can effectively improve cyberspace security. The options of AI systems should be fully utilized in order to achieve the most optimal level of cybersecurity. Lastly, remote working requirements owing to the COVID 19 outbreak have resulted in the value of cloud-based security techniques in protecting and improving the cybersecurity landscape.

V. Conclusion and Future Work

This paper reviews the topic of cyber-attacks focusing on the types and weapons of cyber-attacks, measures and security precautions against cyber-attacks, and the projections of experts on the future of cyber-attacks and the associated security measures.

Interviews were carried with several study participants, delving into the subjects of cybersecurity and cyber-attacks. The information obtained from the participants shows dramatic development of information technology within the past several years. It was found that albeit the presence of precautionary tools, cyber attackers are still successful in breaking the firewall systems, resulting in physical and non-physical damages. Victims of cyber-attacks, especially firms, could lose their reputation as well. Notably, cyber-attack risks and threats appear to increase in tandem with information technology development.

Taking into consideration the present situation of data breaches, ransomware attacks, in addition to the concerns towards the impact of new technologies like AI, and the constantly evolving threats; it is a critical duty of cybersecurity experts to consistently provide the most updated best practices and tools of cybersecurity so that users could consistently avert cyber threats. Equally, employee awareness and expertise on cybersecurity issues need to be encouraged and cultivated via continuous training programs.

Further, scientific research should focus more on security adjustments and measures required by different business sectors and corporations towards remote work that tends to become a necessity today; especially with the spread of Corona pandemic. More focus on individual safety characteristics such as awareness, attitude, behavior and compliance is called for, and research is required to quantify these primary quality indicators. Based on past findings, the human factor appears the key to the progress of information security, but has not been adequately explored.

References

[1] S. Tan, P. Xie, J. M. Guerrero, J. C. Vasquez, Y. Li, and X. Guo, "Attack detection design for dc microgrid using eigenvalue assignment approach," *Energy Reports*, vol. 7, pp. 469–476, 2021.

[2] M. A. Judge, A. Manzoor, C. Maple, J. J. Rodrigues, and S. ul Islam, "Price-based demand response for household load management with interval uncertainty," *Energy Reports*, vol. 7, pp. 8493–8504, 2021.

[3] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[4] G. Aghajani and N. Ghadimi, "Multi-objective energy management in a micro-grid," *Energy Reports*, vol. 4, pp. 218–225, 2018.

[5] I. Priyadarshini, R. Kumar, R. Sharma, P. K. Singh, and S. C. Satapathy, "Identifying cyber insecurities in trustworthy space and energy sector for smart grids," *Computers & Electrical Engineering*, vol. 93, p. 107204, 2021.

[6] J. Al-Gasawneh, A. AL-Hawamleh, A. Alorfi, and G. Al-Rawashde, "Moderating the role of the perceived security and endorsement on the relationship between per-ceived risk and intention to use the artificial intelligence in financial services," *International Journal of Data and Network Science*, vol. 6, no. 3, pp. 743–752, 2022.

[7] H. Akhavan-Hejazi and H. Mohsenian-Rad, "Power systems big data analytics: An assessment of paradigm shift barriers and prospects," *Energy Reports*, vol. 4, pp. 91–100, 2018.

[8] N. Li, C. Tsigkanos, Z. Jin, Z. Hu, and C. Ghezzi, "Early validation of cyber–physical space systems via multi-concerns integration," *Journal of Systems and Software*, vol. 170, p. 110742, 2020.

[9] J. Shin, J.-G. Choi, J.-W. Lee, C.-K. Lee, J.-G. Song, and J.-Y. Son, "Application of stpa-safesec for a cyber-attack impact analysis of npps with a condensate water system test-bed," *Nuclear Engineering and Technology*, vol. 53, no. 10, pp. 3319–3326, 2021.

[10] M. Snehi and A. Bhandari, "Vulnerability retrospection of security solutions for software-defined cyber–physical system against ddos and iot-ddos attacks," *Computer Science Review*, vol. 40, p. 100371, 2021.

[11] A. A. Jamal, A.-A. M. Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using machine learning," *Materials Today: Proceedings*, 2021.

[12] A. M. Hawamleh and A. Ngah, "An adoption model of mobile knowledge sharing based on the theory of planned behavior," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 3-5, pp. 37–43, 2017.

[13] S. W. Brenner, *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press, 2009.

[14] B. Alhayani, S. T. Abbas, D. Z. Khutar, and H. J. Mohammed, "Best ways computation intelligent of face cyber attacks," *Materials Today: Proceedings*, 2021.

[15] A. Hawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, and G. Al-Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," *Solid State Technology*, vol. 63, no. 5, pp. 7894–7899, 2020.

[16] S. Cheung, U. Lindqvist, and M. W. Fong, "Modeling multistep cyber attacks for scenario recognition," in *Proceedings DARPA Information Survivability Conference And Exposition*, vol. 1. IEEE, 2003, pp. 284–292.

[17] I. Frank and E. Odunayo, "Approach to cyber security issues in nigeria: challenges and solution," *International Journal of Cognitive Research in science, engineering and education*, vol. 1, no. 1, pp. 100–110, 2013.

[18] P. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cyber security," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no. 11, pp. 125–128, 2018.

[19] C. O. K. CLN, E. I. C.-K. CLN, I. A. A. O. CLN, and B. A. U. CLN, "Issues on information systems, icts, cyber-crimes, cyber security, cyber ethics, and national security in nigeria: Librarians' research," *Library Philosophy and Practice*, pp. 1–19, 2020.

[20] S. Al-Emadi, A. Al-Mohannadi, and F. Al-Senaid, "Using deep learning techniques for network intrusion detection," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020, pp. 171–176.

[21] L. Griffin, "The effectiveness of cybersecurity awareness training in reducing employee negligence within department of defense (dod) affiliated organizations-qualitative exploratory case study," Ph.D. dissertation, Capella University, 2021.

[22] T. Bhardwaj, H. Upadhyay, and L. Lagos, "Deep learning-based cyber security solutions for smart-city: Application and review," *Artificial Intelligence in Industrial Applications*, pp. 175–192, 2022.

[23] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," *Congressional research service documents, CRS RL32331 (Washington DC)*, vol. 2, 2004.

[24] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Computers & Security*, vol. 60, pp. 154–176, 2016.

[25] K. Thakur, M. L. Ali, S. Kopecky, A. Kamruzzaman, and L. Tao, "Connectivity, traffic flow and applied statistics in cyber security," in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*. IEEE, 2016, pp. 295–300.

[26] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189–208, 2020.

[27] W. Steingartner, D. Galinec, and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," *Symmetry*, vol. 13, no. 4, p. 597, 2021.

[28] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for california's smart inverter functions," in *2019 IEEE CyberPELS (CyberPELS)*. IEEE, 2019, pp. 1–5.

[29] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97–110, 2018.

[30] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137 293–137 311, 2020.

[31] N. Setiawan, V. C. E. Tarigan, P. B. Sari, Y. Rossanty, M. Nasution, and I. Siregar, "Impact of cybercrime in e-business and trust," *Int. J. Civ. Eng. Technol*, vol. 9, no. 7, pp. 652–656, 2018.

[32] T. Holt and A. Bossler, *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge, 2015.

[33] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *The economics of information security and privacy*. Springer, 2013, pp. 265–300.

[34] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *Journal in computer virology*, vol. 2, no. 1, pp. 13–20, 2006.

[35] A. C. Moise *et al.*, "A few comments on the council of europe convention on cybercrime," *Jurnalul de Drept si Stiinte Administrative*, vol. 2, no. 8, pp. 28–38, 2017.

[36] N. C. Hampson, "Hacktivism: A new breed of protest in a networked world," *BC Int'l & Comp. L. Rev.*, vol. 35, p. 511, 2012.

[37] T. U. Rehman, "Psychosocial aspects of cybercrime victimization in pakistan," in *Handbook of Research on Applied Social Psychology in Multiculturalism*. IGI Global, 2021, pp. 192–211.

[38] D. Shivpuri, "Cyber crime: Are the law outdated for this type of crime," *International Journal of Research in Engineering, Science and Management*, vol. 4, no. 7, pp. 44–49, 2021.

[39] A. Sarmah, R. Sarmah, and A. J. Baruah, "A brief study on cyber crime and cyber law's of india," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 6, pp. 1633–1640, 2017.

[40] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, pp. 65–88, 2015.

[41] C. Ventures, "2019 official annual cybercrime report," in *Recuperado el*. Herjavec Group, 2019.

[42] R. Fisher, C. Porod, and S. Peterson, "Motivating employees and organizations to adopt a cybersecurity-focused culture," *Journal of Organizational Psychology*, vol. 21, no. 1, pp. 114–131, 2021.

[43] A. Al-Marghilani, "Comprehensive analysis of iot malware evasion techniques," *Engineering, Technology & Applied Science Research*, vol. 11, no. 4, pp. 7495–7500, 2021.

[44] A. Goel, D. K. Sharma, and K. D. Gupta, "Leobat: Lightweight encryption and otp based authentication technique for securing iot networks," *Expert Systems*, vol. 39, no. 5, p. e12788, 2022.

[45] Y. E. Suzuki and S. A. S. Monroy, "Prevention and mitigation measures against phishing emails: a sequential schema model," *Security Journal*, vol. 35, no. 4, pp. 1162–1182, 2022.

[46] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629–3654, 2017.

[47] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[48] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, "Dos and ddos attacks: defense, detection and traceback mechanisms-a survey," *Global Journal of Computer Science and Technology*, 2014.

[49] S. Shalini and S. Usha, "Prevention of cross-site scripting attacks (xss) on web applications in the client side," *International Journal of Computer Science Issues (IJCSI)*, vol. 8, no. 4, p. 650, 2011.

[50] M. Souppaya, K. Scarfone *et al.*, "Guide to malware incident prevention and handling for desktops and laptops," *NIST Special Publication*, vol. 800, p. 83, 2013.

[51] A. Sheikh, "Trojans, backdoors, viruses, and worms," in *Certified Ethical Hacker (CEH) Preparation Guide*. Springer, 2021, pp. 49–69.

[52] S. Sharma, "Design and implementation of malware detection scheme." *International Journal of Computer Network & Information Security*, vol. 10, no. 8, 2018.

[53] M. Rai and H. Mandoria, "A study on cyber crimes cyber criminals and major security breaches," *Int. Res. J. Eng. Technol.*, vol. 6, no. 7, pp. 1–8, 2019.

[54] B. Narwal, A. K. Mohapatra, and K. A. Usmani, "Towards a taxonomy of cyber threats against target applications," *Journal of Statistics and Management Systems*, vol. 22, no. 2, pp. 301–325, 2019.

[55] I. A. Chesti, M. Humayun, N. U. Sama, and N. Jhanjhi, "Evolution, mitigation, and prevention of ransomware," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. IEEE, 2020, pp. 1–6.

[56] K. K. Gagneja, "Knowing the ransomware and building defense against it-specific to healthcare institutes," in *2017 Third International Conference on Mobile and Secure Services (MobiSecServ)*. IEEE, 2017, pp. 1–5.

[57] M. Papoutsakis, K. Fysarakis, G. Spanoudakis, S. Ioannidis, and K. Koloutsou, "Towards a collection of security and privacy patterns," *Applied Sciences*, vol. 11, no. 4, p. 1396, 2021.

[58] S. Boonkrong, "Methods and threats of authentication," in *Authentication and Access Control*. Springer, 2021, pp. 45–70.

[59] A. Kanta, S. Coray, I. Coisel, and M. Scanlon, "How viable is password cracking in digital forensic investigation? analyzing the guessability of over 3.9 billion real-world accounts," *Forensic Science International: Digital Investigation*, vol. 37, p. 301186, 2021.

[60] R. Beno and R. Poet, "Hacking passwords that satisfy common password policies: Hacking passwords," in *13th International Conference on Security of Information and Networks*, 2020, pp. 1–3.

[61] V. Nithya, S. L. Pandian, and C. Malarvizhi, "A survey on detection and prevention of cross-site scripting attack," *International Journal of Security and Its Applications*, vol. 9, no. 3, pp. 139–152, 2015.

[62] A. M. K. Alhawamleh, "Web based english placement test system (elpts)," Ph.D. dissertation, Universiti Utara Malaysia, 2012.

[63] A. Raman, S. Kaushik *et al.*, "A comprehensive study of contemporary tools and techniques in the realm of cyber security," *IITM Journal of Management and IT*, vol. 7, no. 1, pp. 108–120, 2016.

[64] J. L. Duffany, "Computer security," in *Computer and Network Security Essentials*. Springer, 2018, pp. 3–20.

[65] K. Kallepalli and U. B. Chaudhry, "Intelligent security: Applying artificial intelligence to detect advanced cyber attacks," in *Challenges in the IoT and Smart Environments*. Springer, 2021, pp. 287–320.

[66] M. Chakraborty and M. Singh, "Introduction to network security technologies," in *The" Essence" of Network Security: An End-to-End Panorama*. Springer, 2021, pp. 3–28.

[67] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *The journal of supercomputing*, vol. 76, no. 12, pp. 9493–9532, 2020.

[68] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? revealing the nuts and bolts of the security of mobile devices," in *2011 IEEE Symposium on Security and Privacy*. IEEE, 2011, pp. 96–111.

[69] R. P. Jover, "Security analysis of sms as a second factor of authentication," *Communications of the ACM*, vol. 63, no. 12, pp. 46–52, 2020.

[70] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A survey on the cryptographic encryption algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 11, 2017.

[71] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *2017 international conference on engineering and technology (ICET)*. IEEE, 2017, pp. 1–7.

[72] N. G. Kumar and K. K. Rao, "Hash based approach for providing privacy and integrity in cloud data storage using digital signatures," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 6, pp. 8074–8078, 2014.

[73] D. Hofheinz and T. Jager, "Tightly secure signatures and public-key encryption," *Designs, Codes and Cryptography*, vol. 80, no. 1, pp. 29–61, 2016.

[74] J. Malzac, "Leveraging domestic law against cyberattacks," *Nat'l Sec. L. Brief*, vol. 11, p. 1, 2021.

[75] B. Pranggono and A. Arabo, "Covid-19 pandemic cybersecurity issues," *Internet Technology Letters*, vol. 4, no. 2, p. e247, 2021.

[76] F. Schlackl, N. Link, and H. Hoehle, "Antecedents and consequences of data breaches: A systematic review," *Information & Management*, p. 103638, 2022.

[77] P. Langlois, "2020 data breach investigations report," *Verizon*, 2020.

[78] M. Jartelius, "The 2020 data breach investigations report–a cso's perspective," *Network Security*, vol. 2020, no. 7, pp. 9–12, 2020.

[79] K. Raghavan, M. S. Desai, and P. Rajkumar, "Managing cybersecurity and ecommerce risks in small businesses," *Journal of management science and business intelligence*, vol. 2, no. 1, pp. 9–15, 2017.

[80] P. Lorenzo, F. Stefano, A. Ferreira, and P. Carolina, "Artificial intelligence and cybersecurity: Technology, governance and policy challenges," 2021.

[81] H. Lee and K.-S. Choi, "Interrelationship between bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework," *Victims & Offenders*, vol. 16, no. 3, pp. 363–384, 2021.

[82] Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, and A. K. Jaiswal, "A systematic literature review on the cyber security," *International Journal of scientific research and management*, vol. 9, no. 12, pp. 669–710, 2021.

[83] S. Gangwar and V. Narang, "A survey on emerging cyber crimes and their impact worldwide," in *Research Anthology on Combating Cyber-Aggression and Online Negativity*. IGI Global, 2022, pp. 1583–1595.

[84] N. Hassan, *Ransomware Revealed*. Springer, 2019.

[85] W. Crumpler and J. A. Lewis, *The cybersecurity workforce gap*. Center for Strategic and International Studies (CSIS) Washington, DC, USA, 2019.

[86] A. Kanaan, A. AL-Hawamleh, A. Abulfaraj, H. Al-Kaseasbeh, and A. Alorfi, "The effect of quality, security and privacy factors on trust and intention to use e-government services," *International Journal of Data and Network Science*, vol. 7, no. 1, pp. 185–198, 2023.

[87] T. C. Truong, I. Zelinka, J. Plucar, M. Čandík, and V. Šulc, "Artificial intelligence and cybersecurity: Past, presence, and future," in *Artificial intelligence and evolutionary computations in engineering systems*. Springer, 2020, pp. 351–363.